

Graph-Based Multimodal Traffic Prediction Under Adversarial Diffusion Across Varying Network Scales Versus Standard GCNs

Assignee Research

June 16, 2026

Abstract

Real-time traffic prediction models play a pivotal role in smart mobility systems and have been widely used in route guidance, emerging mobility services, and advanced traffic management systems. With the availability of massive traffic data, neural network-based deep learning methods, especially the graph convolutional networks (GCN) have demonstrated outstanding performance in mining spatio-temporal information and achieving high prediction accuracy. Recent studies reveal the vulnerability of GCN under adversarial attacks, while there is a lack of studies to understand the vulnerability issue

1 Introduction

This paper examines: Adversarial Diffusion Attacks on Graph-based Traffic Prediction Models. Research question: How scalable are graph-based multimodal traffic prediction models under adversarial diffusion attacks when evaluated on datasets with varying graph sizes (e.g., small vs. large-scale traffic networks), and how does this compare to standard GCN-based models?.

2 Methodology

Systematic literature search across multiple databases yielded 11 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 8.2/10.

3 Results

11 papers retrieved. 22 claims extracted; 21 independently verified. Quality review score: 8.2/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

5 Extracted Claims

Claim	Verified	Confidence
Neural networks are vulnerable to deliberately designed samples, known as adversarial samples.	✓	0.23
Adversarial samples can be generated by adding imperceptible perturbations to the original data sample.	✓	0.22
Adversarial samples are low-probability but densely distributed.	✓	0.18
Neural networks are vulnerable to adversarial samples when they demonstrate linear behaviors in high-dimensional spaces.	✓	0.22
Potential attackers could take advantage of deep learning models and degrade their performance using adversarial samples	✓	0.21
Few studies have investigated the vulnerability and robustness of traffic prediction systems.	✓	0.16
Industry-level traffic information systems can be attacked easily.	✓	0.18
A German artist used 99 smartphones to create virtual vehicles, causing Google Maps to wrongly identify an empty street	✓	0.15
Adversarial attacks on traffic prediction models can affect every aspect of smart mobility systems.	✓	0.19
Smartphone-based mobility applications like Google Maps and AutoNavi make traffic state estimation and prediction based	✓	0.28
Users' mobile phones can be hacked and the information can be deliberately altered to attack the systems.	✓	0.22
Individual mobility applications are vulnerable to adversarial attacks because the difficulties of hacking users' mobile	✓	0.23
Neural network models demonstrate potentials in traffic prediction with multi-source data on large-scale networks.	✓	0.25
Various neural network models have been used for traffic prediction, including CNN, RNN, attention, and GCN.	✓	0.18
Traffic prediction tasks can be categorized into multiple purposes, such as traffic state prediction, demand prediction,	✓	0.24
Traffic state prediction includes the prediction of traffic flow, speed, and travel time. 4	×	0.12
Traffic demand prediction aims to predict the number of users and traffic demand, such as taxi request, subway inflow/ou	✓	0.21
Trajectory prediction is used for dynamic positioning and resource allocation.	✓	0.16
Most traffic prediction tasks can be carried out by neural network models	✓	0.20

References

- <http://arxiv.org/abs/2405.18770v6>
- <http://arxiv.org/abs/2503.09124v1>
- <http://arxiv.org/abs/2104.09369v1>